REMARKS

Claims 1-49 were pending in the application. Claims 14-18, 34-37, and 41-49 have been withdrawn from consideration. Claims 10 and 31 have been cancelled. Claims 1-9, 11-13, 19-30, 32-33, and 38-40 remain pending and under consideration in the application.

Restriction Requirement:

Applicant acknowledges the restriction requirement to the claims of species (1a), as discussed between the Examiner and the undersigned on February 9, 2007. Thus, in addition to previously withdrawn claims 41-49, claims 14-18 and 34-37 are also withdrawn from further consideration by the Examiner as being drawn to non-elected species.

35 U.S.C. § 103(a) Requirements:

Claims 1-9, 11-13, 19-30, 32-33, and 38-40 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Matthews, U.S. Patent Application Publication 2003/0044007. Claims 10 and 31 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Matthews in view of Lai, U.S. Patent 5,485,619. Applicant respectfully traverses these rejections.

The cited references, taken singly or in combination, fail to teach or suggest all of the elements of the independent claims. Matthews teaches "[m]ethods and apparatus [are provided] for improving ARC4 processing in a cryptography engine. A multiple ported memory can be used to allow pipelined read and write access to values in memory. Coherency checking can be applied to provide that read-after-write and write-after-write consistency is maintained. Initialization of the memory can be improved with a reset feature occurring in a single cycle. Key shuffle and key stream generation can also be performed using a single core." (Abstract, Matthews).

Lai teaches "[a] subscript table mapping system for optimizing the compilation of certain Fortran 90 array construction and array manipulation transformation functions.

The subscript table data object of this invention is used to perform the three compiler optimizations, including subscript dependency analysis, subscript table transformation and optimized code generation. Application of a simple subscript mapping function tailored to the particular intrinsic Fortran 90 array variable transformation function permits compilation of executable binary code that saves substantial processing steps and data storage space by avoiding during execution the usual requirement for temporary storage of abstract transformational array variables." (Abstract, Lai).

In contrast, Applicant's independent claim 1 recites, in pertinent part:

"A method of encrypting information, the method comprising:
in a first pipeline stage:
obtaining a value *A* from an array having a plurality of values ,
wherein each of the values is stored in a corresponding one
of a plurality of storage locations; and
determining a value *B* based on the value *A*; ...
wherein the method further comprises:
shifting the array to enable the value *A* to be obtained from the same one
of the plurality of storage locations in the array for each iteration;
and
obtaining the value *A* from the same one of the plurality of storage
locations for each iteration" (Emphasis added).

Independent claim 22 recites a similar combination of features.

Neither Matthews or Lai, taken singly or in combination, teach or suggest "shifting the array to enable the value *A* to be obtained from the same one of the plurality of storage locations in the array for each iteration; and obtaining the value A from the same one of the plurality of storage locations for each iteration" as recited in combination with the other features of independent claim 1. In the office action, the Examiner acknowledges that Matthews does not disclose shifting the array each iteration. The

Examiner contends that Lai discloses that iterative computations (DO-loop), which involve incrementing an array index, are implemented by shifting the array each iteration, citing Lai at Col. 14, lines 11-21. However, Lai does not teach or suggest "shifting the array to enable the value *A* to be obtained from the **same one** of the plurality of storage locations in the array for each iteration" as recited in combination with the other features of claim 1, and similarly recited in independent claim 22. Furthermore, neither Matthews nor Lai provide any teaching or suggestion, regarding "obtaining the value *A* from the same one of the plurality of storage locations for each iteration" whether taken singly or in combination together.

In light of the above, Applicant submits that a case of obviousness has not been established, and respectfully requests removal of the 35 U.S.C. § 103(a) rejections.

CONCLUSION

Applicants submit the application is in condition for allowance, and an early notice to that effect is requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5681-64400/EAH.

Respectfully submitted,

Erik A. Heter
Reg. No. 50,652
AGENT FOR APPLICANT(S)

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8800

Date: 5/22/07